Long Range 802.11b/g/n USB Adapter for Outdoor Use

Model: ARK-2404U-3

User Manual

Revision 1.0

Note	***Make sure there are antennas installed on each unit, otherwise the RF will be damaged when power is on.***

FCC Notice

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacture is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user’s authority to operate the equipment.

Introduction

The ARK-2404U-3 wireless network adapter is a powerful 32-bit USB Adapter that installs quickly and easily into PCs or Notebook. This adapter can be used in Ad-Hoc mode to connect with a wireless access point or router for access to the internet in your enterprise or home network.

ARK-2404U-3 wireless USB adapter connects you with 802.11n networks at up to a 150Mbps. And for added versatility, it can also interoperate with all 802.11g (up to 54Mbps) and 802.11b (up to 11Mbps) products found in homes, business, and public wireless hotspots around the country. And in either mode, your wireless communications are protected by industrial-strength WPA/WPA2, so your data stays secured.

This manual contains information of how to install and configure your wireless adapter to get your network started accessing the internet. It will guide you through the correct configuration steps to get your device up and running.

Before you begin

You must have at least the following:

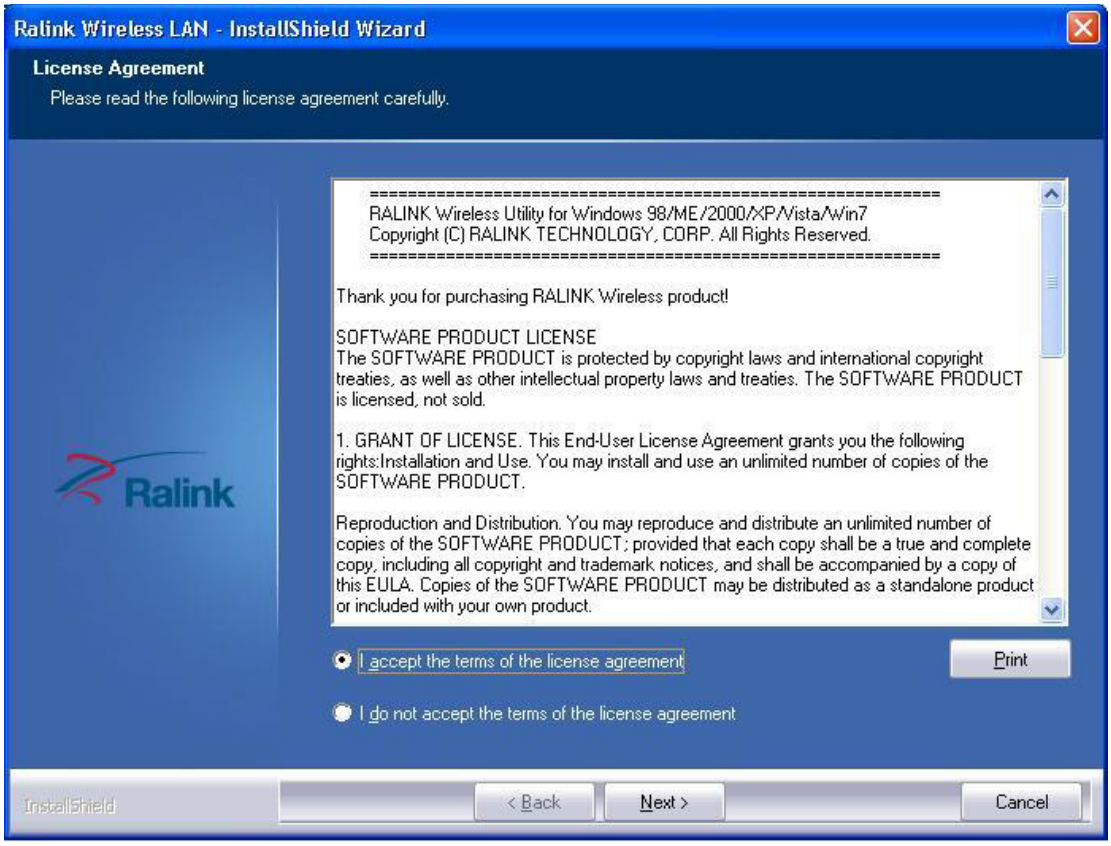
- A laptop computer / Desktop PC with an available 32-bit USB port
- At least a 300MHz processor and 32MByte of memory
- Windows 2000 / XP 32-64 / Vista 32-64 / Windows 7 32-64 / Macintosh / Linux
- A CD-ROM drive

Installing drivers and utilities

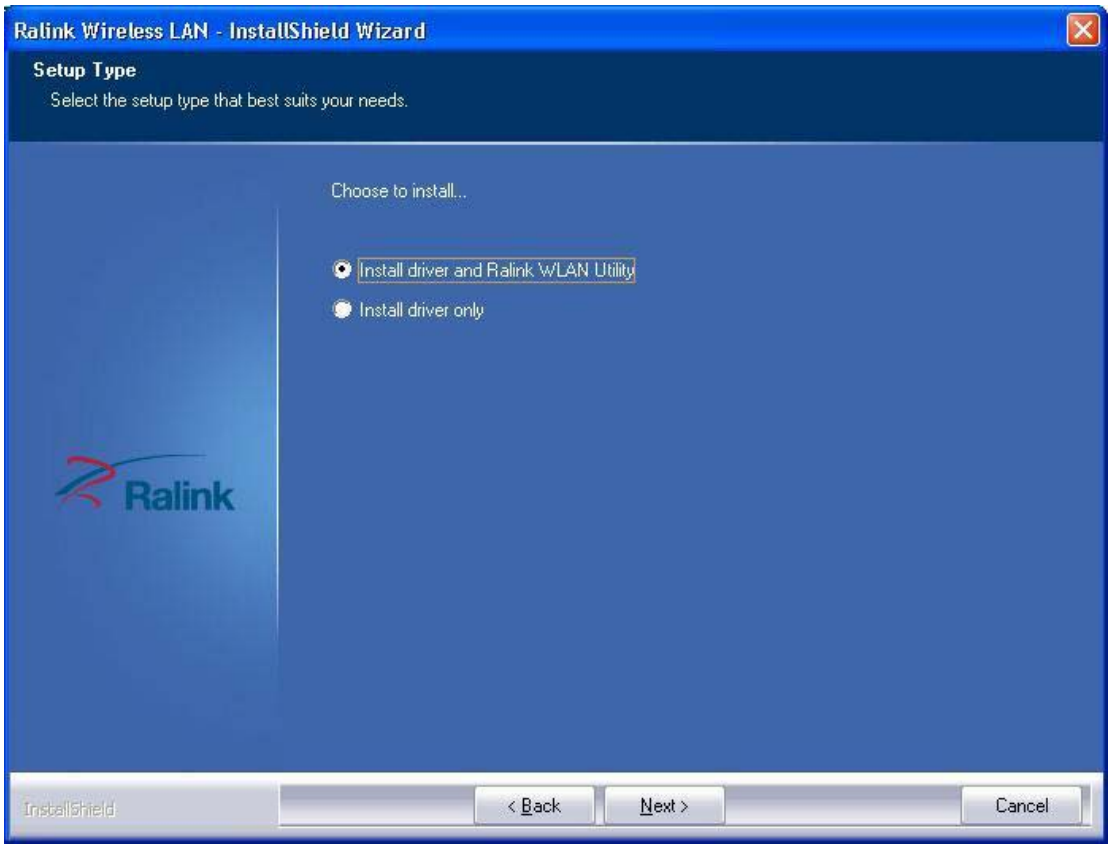
1. Do not connect the adapter to your computer.
2. Insert the driver and utility CD in the CD-ROM drive.
3. The setup wizard will launch automatically (under Windows Vista/7, you may additionally need to select **Run: Autorun.exe** in the Autorun window). If the CD-ROM autorun feature is disable. Run **Autorun.exe** in the CD's root directory.
4. Click Install **Driver/Utility** for your adapter. If you are using Windows Vista, the User Account Control window may display. To proceed with the installation,

click **Continue** (if you are performing the installation using an account that has no administrative privileges, you may also need to enter the user name and password for an administrative account).

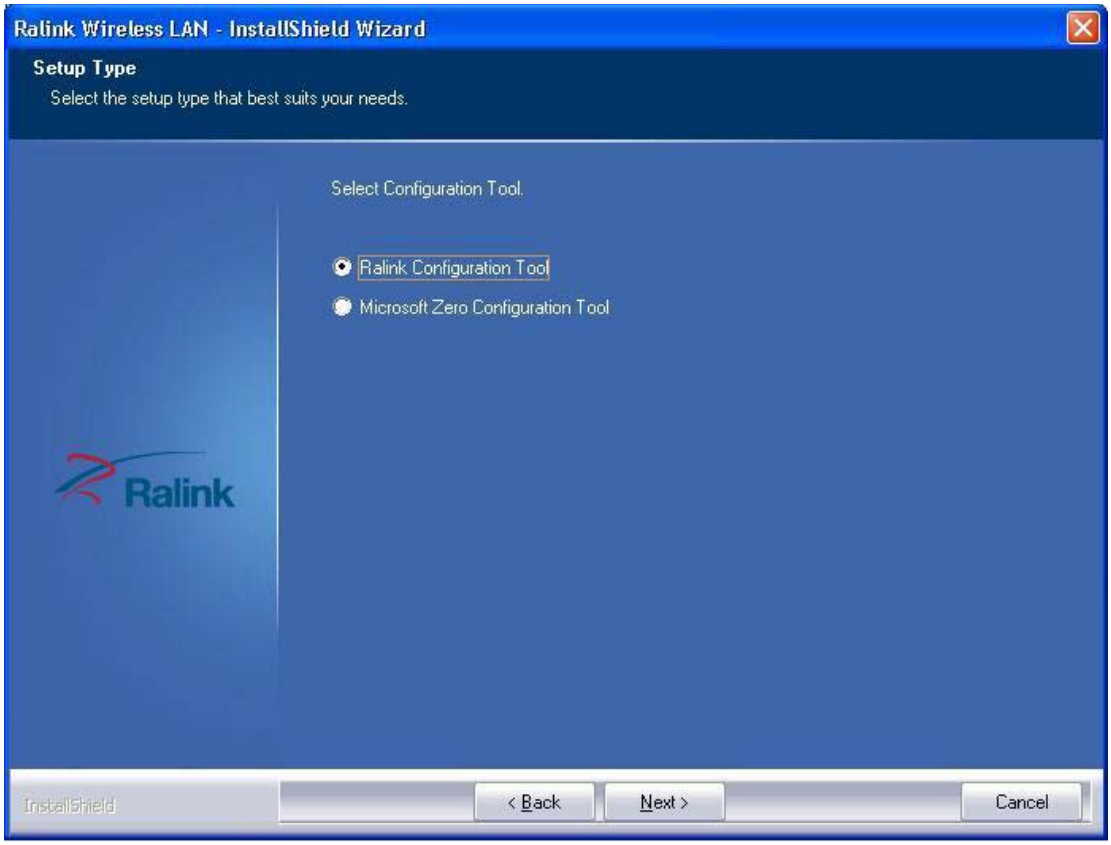
5. Select **I accept the terms of the license agreement** and click **Next>.**

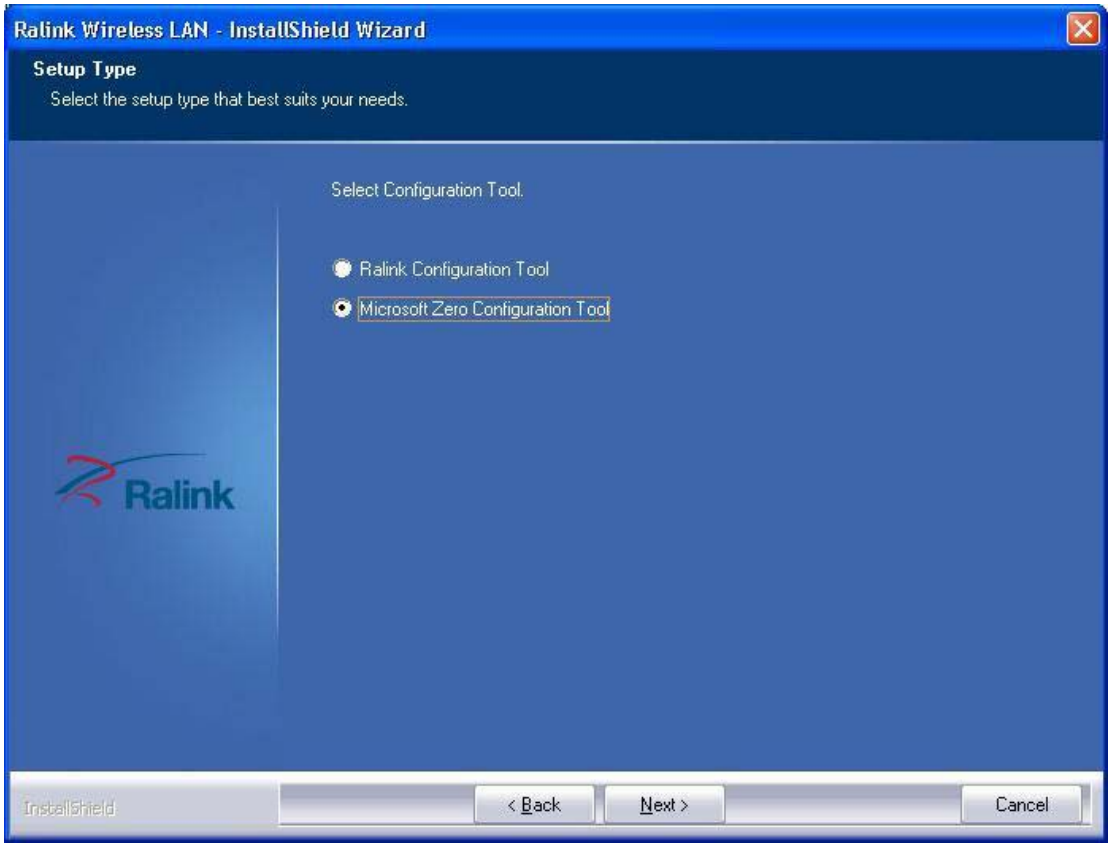

Ralink Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
RALINK Wireless Utility for Windows 98/ME/2000/XP/Vista/Win7
Copyright (C) RALINK TECHNOLOGY, CORP. All Rights Reserved.
Thank you for purchasing RALINK Wireless product!
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
Ralink
InstallShield
< Back
Next >
Cancel

6. If you wish to install the driver with utility software (recommended), select **Install driver and Ralink WLAN Utility**. If you wish to install driver only, click **Install driver only** and click **Next>.**

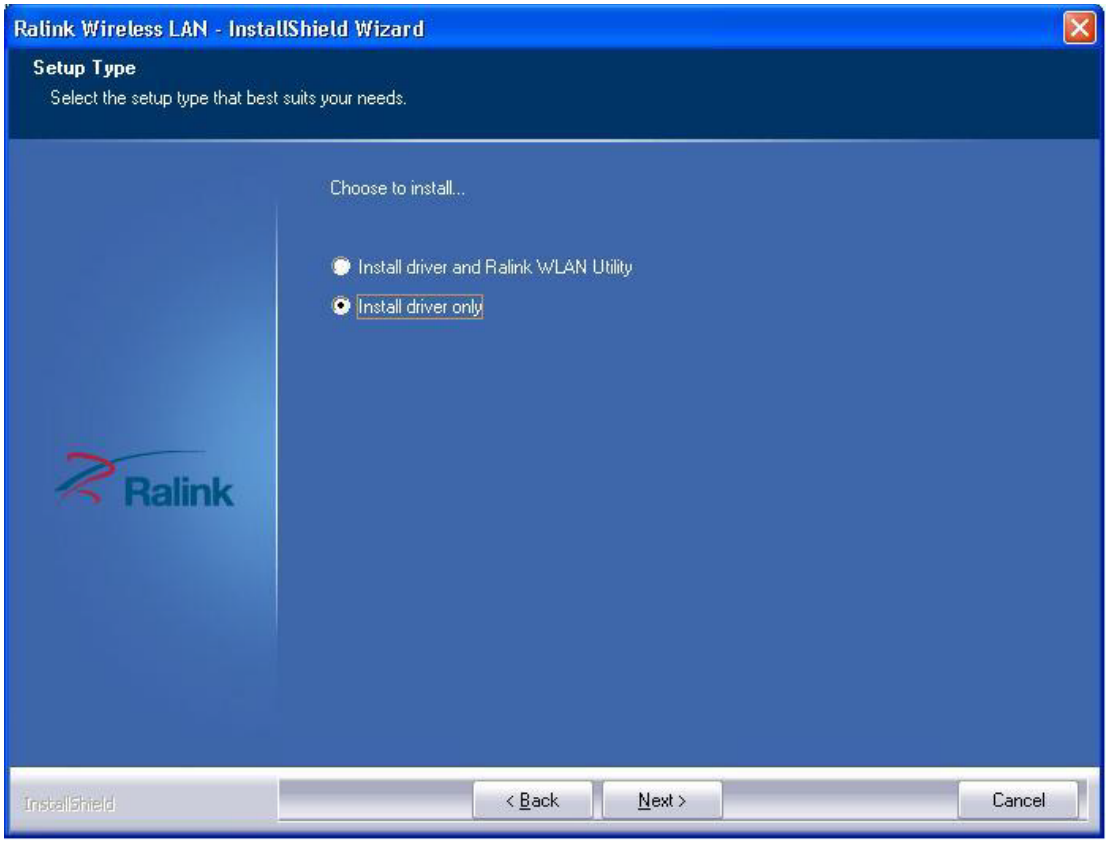


7. If you wish to use the software included with the adapter (recommended), select **Install driver and Ralink Configuration Tool** and click **Next>**. If you wish to use your system's wireless network wizard, select **Microsoft Zero Configuration Tool** and click **Next>**.


Ralink Wireless LAN - InstallShield Wizard
Setup Type
Select the setup type that best suits your needs.
Select Configuration Tool.
Ralink Configuration Tool
Microsoft Zero Configuration Tool
Ralink
InstallShield
< Back
Next >
Cancel

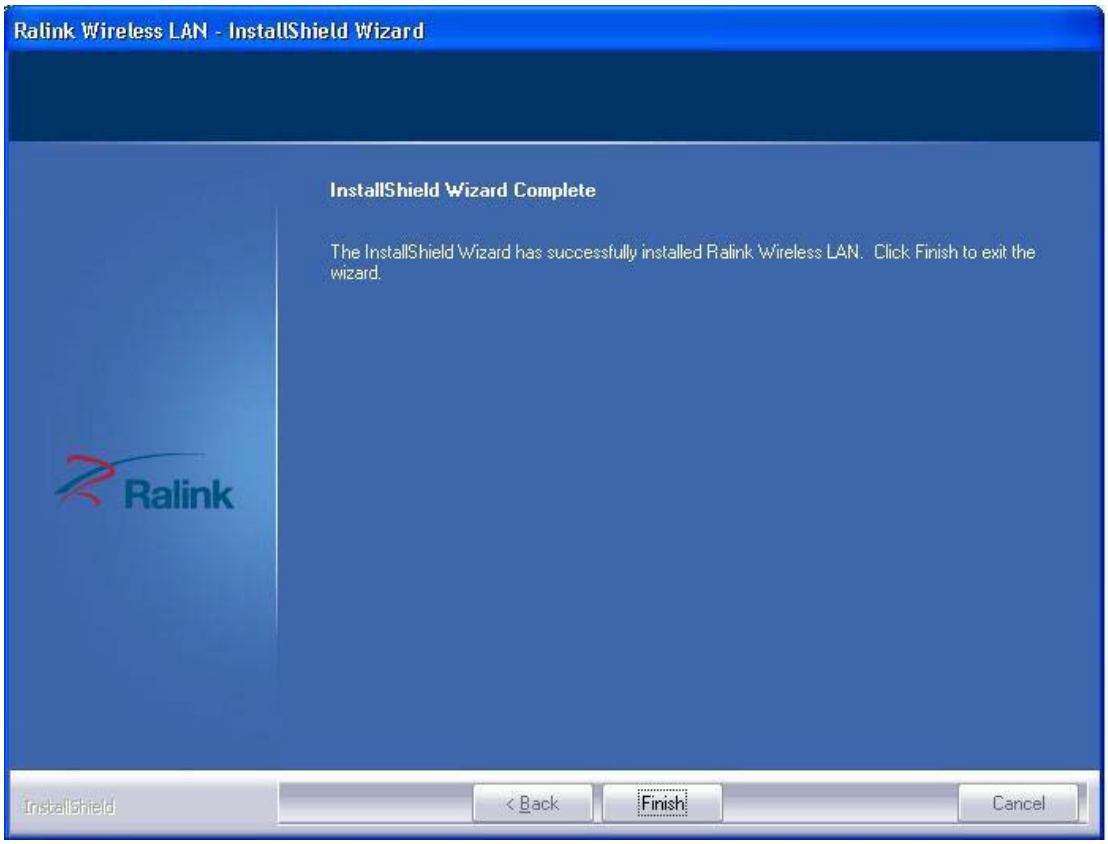

Ralink Wireless LAN - InstallShield Wizard
Setup Type
Select the setup type that best suits your needs.
Select Configuration Tool.
Ralink Configuration Tool
Microsoft Zero Configuration Tool
Ralink
InstallShield
< Back
Next >
Cancel

8. Click **Install** to install the driver and configuration utility.



9. If a restart is required, select **Yes** to restart my computer now to restart the computer after the installation or select **No** to restart the computer at a later time. Click **Finish** to complete the setup wizard.

System Settings Change
Windows has finished installing new devices. The software that supports your device requires that you restart your computer.You must restart your computer before the new settings will take effect.
Do you want to restart your computer now?
Yes
No


Ralink Wireless LAN - InstallShield Wizard
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed Ralink Wireless LAN. Click Finish to exit the wizard.
Ralink
InstallShield
< Back
Finish
Cancel

Installing the adapter

1. Turn on the computer and wait for the operating system to launch. Log in, if necessary.
2. Plug the adapter into a USB port.
3. If the Found New Hardware Wizard window appears, select **Install the software automatically** (recommended) and click **Next**. The driver will be installed automatically.

Wireless adapter configuration

A configuration application is installed with adapter drivers. The application's icon is displayed in the system tray (next to the clock), and its appearance depends on the adapter and/or connection status.

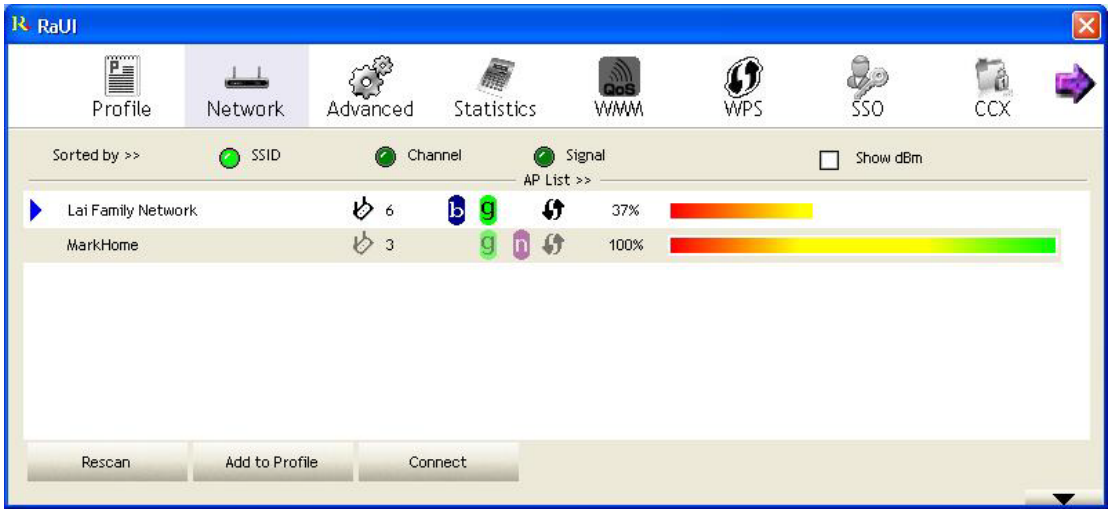
The adapter is not attached to the PC or RF is off.	The adapter is not connected to a wireless network.	The adapter is connected to a wireless network.

To launch the adapter's configuration, double-click the application's icon (**RaUI**).

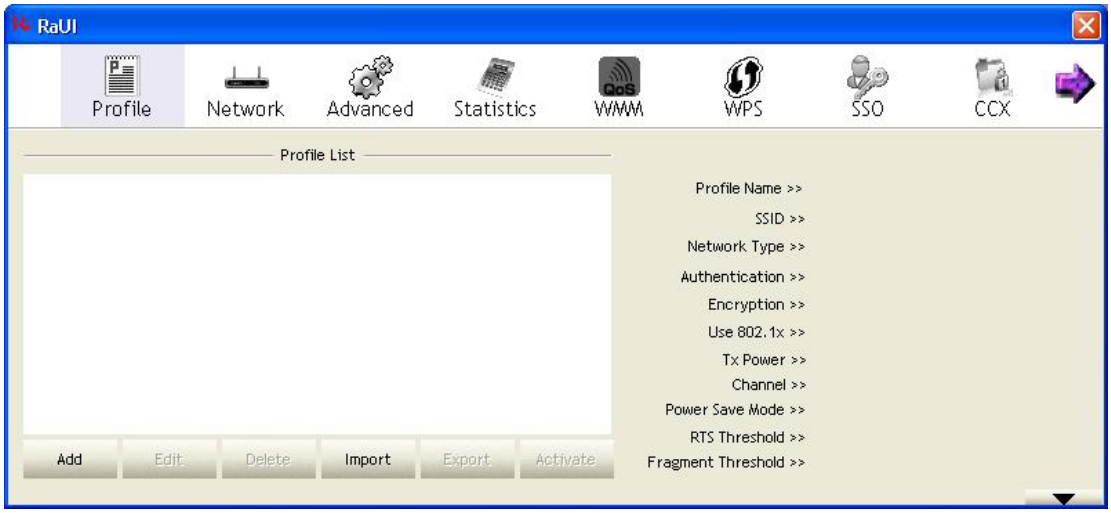
RaUI application

RaUI application window is divided into three parts:

1. Tab bar – click on Tab to display its contents in the main pane. Active Tab is highlighted.



2. Main pane – this pane displays contents of select Tab.



3. Secondary pane – this pane contains connection information or additional options for selected in main pane option. Click More (▼) button to show secondary pane or Less (▲) button to hide it.
   Connection information contains:
   Status – Connection status:
   - RF OFF – Adapter disconnected or RF is off.
   - Disconnected – Wireless connection not established.
   - 〔SSID〕< -- > 〔BSSID〕– Connection established to network with displayed ID's.

   Extra info – Additional information about connection.
   Channel – Channel (Frequency) used by wireless network.
   Authentication –Authentication method by wireless network.

Encryption–Encryption method by wireless network.
Network Type:

- Ad hoc–Connection peer to peer with other wireless adapter.
- Infrastructure–Connection with wireless network via Access Point (AP) or wireless router.

Status–Wireless connection status.
IP Address–IP address configured or obtained from DHCP server.
Subnet Mask–Subnet Mask configured or obtained from DHCP server.
Default Gateway–Gateway IP address configured or obtained from DHCP server.
Link Quality: Shows link quality as a percentage bar (0~100%).
Signal Strength: Shows signal strength as a percentage bar (0~100%).
Noise Level: Shows noise level as a percentage bar (0~100%).
Transmit / Receive: Transmit / Receive as a percentage bar (0~100%).

Profile Tab

This Tab allows you to create profiles for the most frequently used wireless network, i.e. home network, company network or public hotspots. The profile can be activated as required.

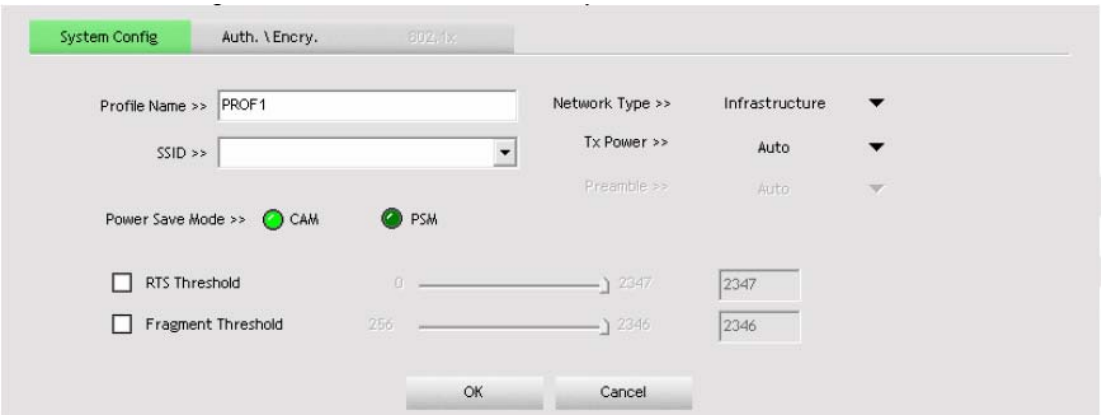
Profile List –This list contains configured profiles, profile name, SSID, information. Icons on the list means as below:

	Connection with activated profile established successfully
	Connection with activated profile not established
	Infrastructure Type network
	Ad hoc Type network
	Secured network

Add: Click **Add** to create a new profile.
Edit: Click **Edit** to change settings for the selected profile.
Delete: Click **Delete** to delete the selected profile.
Activate: Click **Activate** to activate the selected profile.

Profile configuration – System Config Tab

This Tab allows configuration of basic connection parameters.



Profile Name – Enter a name to identify your profile. Default is **PROF1**.

SSID –Enter a network service set identifier (SSID) or select from a list of active networks. If SSID broadcast function of AP is disabled, SSID must be entered manually.

Network Type – You can select two wireless network types:

- The **Infrastructure** mode supports communications between a wireless network and a wire network using an access point.
- The **Ad hoc** mode supports peer to peer communications between two wireless network devices.

TX Power – Set the signal transmit power to be used by the radio transmitter. Choose the appropriate value from the drop-down list.

Preamble –Select the preamble length, default is **Auto**.

Channel –Select the channel to be used when establishing an Ad hoc network.

Power Save Mode –Select the power saving mode.

- Using **CAM** (Constantly Awake Mode), the network adapter will operate at full power when connected to mains.
- Using **PSM** (Power Saving Mode), the network adapter will enter power saving mode.

RTS Threshold –Use the slider or enter a value for the RTS threshold in the field provided. Default value: **2347**.

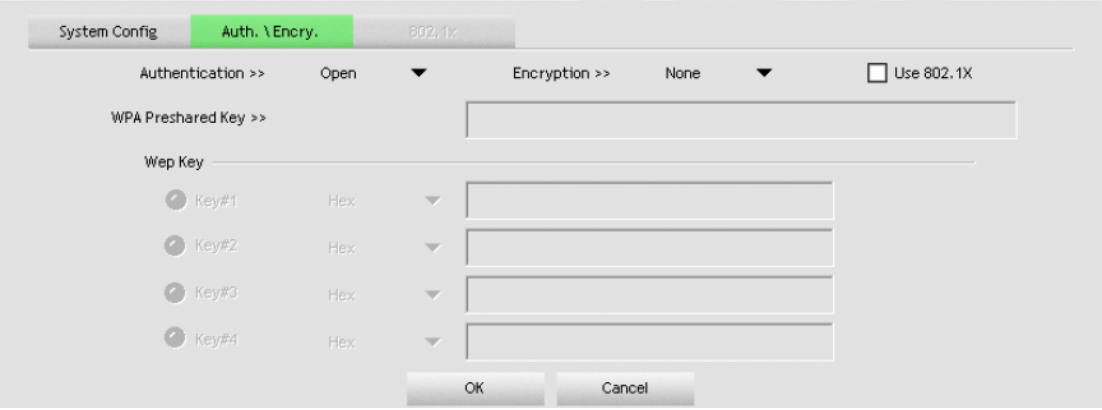
Fragment Threshold –Use the slider or enter a value for the fragment threshold in the field provided. Default value: **2346**.

Profile configuration – Auth. \ Encry. Tab

This Tab contains all Authentication and Encryption settings

Authentication:

- **Open** –With the **Open** method, every wireless station can request authentication.
- **Shared** –With the **Shared** authentication, the station requesting authentication must provide a secret key (which can be obtained from network administrator) using a secure channel (independent of the 802.11 wireless communications channel).
- **LEAP** –(Light Extensible Authentication Protocol) is an EAP authentication method used primarily on Cisco Aironet wireless networks. This protocol encrypts transmitted data using dynamically generated WEP keys, and supports two way authentications.
- **WPA** and **WPA2** –IEEE 802.1x protocol is used for authentication and AES or TKIP for encryption.
- **WPA PSK** and **WPA2 PSK**–Station requesting authentication must provide a WPA Preshared Key. AES or TKIP are used for encryption.
- **Authentication: Open and Shared**



Authentication –Change authentication method.

Encryption –Select **None** or **WEP**.

Use 802.1x –Check this option to use IEEE 802.1x for authentication. IEEE 802.1x supports full user authentication and control. This will also enable 802.1x Tab, where 802.1x can be configured.

WEP Key / Key#1 …4 –When you select **WEP** encryption or **Shared** authentication without 802.1x, you need to enter a correct WEP key.

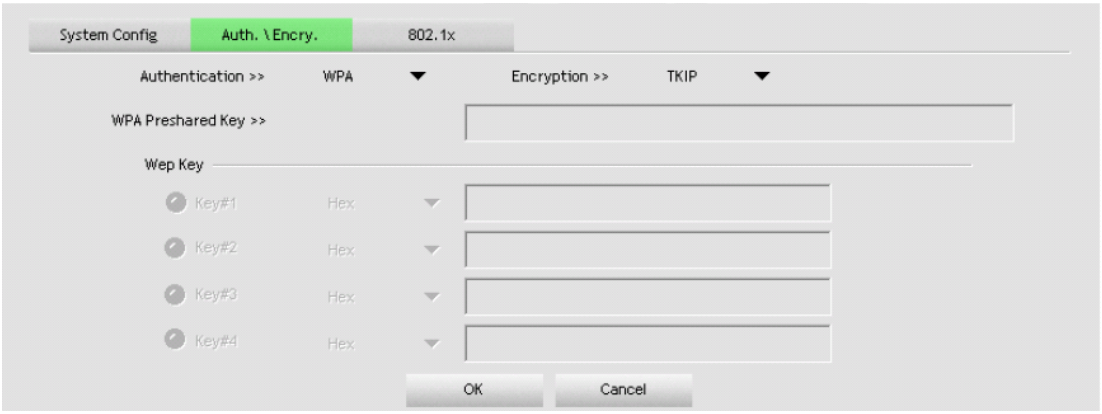
- If a 64-bit WEP key is used, enter 10 **Hexadecimal** characters or 5

ASCII characters.

- If a 128-bit WEP key is used, enter 26 **Hexadecimal** characters or 13 **ASCII** characters.
- **Authentication: LEAP**

Authentication –Change authentication method.
Identity –Enter your identity for the LEAP authentication service.
Password –Enter your password for the LEAP authentication service.
Domain Name –Enter your domain name for the LEAP authentication service.

- **Authentication: WPA and WPA2**

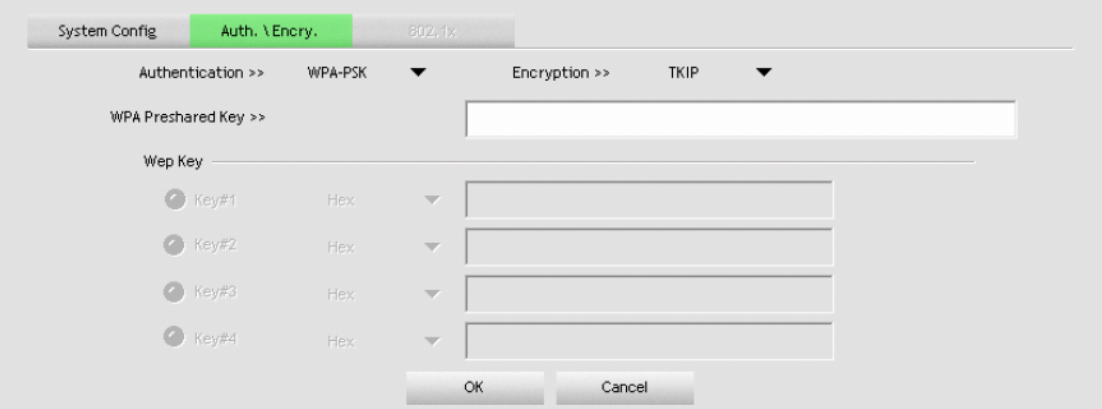


Authentication –Change authentication method.
Encryption –Select the encryption method to be used.

- **AES** (Advanced Encryption System) uses symmetrical 128-bit data block encryption.
- **TKIP** (Temporal Key Integrity protocol) uses stronger encryption algorithms and MIC (Message Integrity Check) to provide security against hackers.

WPA and WPA2 use IEEE 802.1x protocol for authentication. After selecting encryption method go to 802.1x Tab, where 802.1x settings can be configured.

- **Authentication: WPA-PSK and WPA2 PSK**



Authentication –Change authentication method.

Encryption –Select the encryption method to be used.

- **AES** (Advanced Encryption System) uses symmetrical 128-bit data block encryption.
- **TKIP** (Temporal Key Integrity protocol) uses stronger encryption algorithms and MIC (Message Integrity Check) to provide security against hackers.

WPA Preshared Key –Enter the WPA preshared key (WPA-PSK and WPA2-PSK only). The key should be 8 to 32 characters in length.

Profile configuration – 802.1x Tab

Settings on this Tab allow IEEE 802.1x protocol. All information can be obtained from wireless network administrator. Appearance of this Tab depends on options selected from **EAP method** and **Tunnel Authentication** lists.

- **PEAP** –Protect Extensible Authentication Protocol. PEAP transports secured authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of secure wireless network.
- **TLS/Smart Card** –Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the AP.
- **TTLS** –Tunnel Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS, it requires only server-side certificates.
- **EAP-FAST** –Flexible Authentication via secured Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed on time) to the client either manually or automatically. Manual provisioning is delivered to the client via disk or secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only support “Generic Toke Card” authentication now.
- **MD5-Challenge** –Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication, there is no mutual authentication of wireless client and the network.

- **ID\PASSWORD Tab**

EAP Method –Change EAP authentication method.

Tunnel Authentication –Change tunnel authentication method.

Session Resumption –Enable/disable session resumption.

Authentication ID / Password –**Identity**, **Password** and **Domain Name** for server. Only **EAP-FAST** authentication can key in domain name. Domain name can be keyed in blank space.

Tunnel ID / Password:

- **Identity** –Identity for tunnel.
- **Password** –Password for tunnel.

Client Certificate Tab

Use Client certification –Enable this option to use Client certificate for server authentication and then select certificate from drop-down list. You can find detailed information on certificate below this list.

Server Certificate Tab

Use certificate chain –Enable this option, to enable the certification feature and select the certificate issue.

Allow intermediate certificates –Select this option to allow the use of intermediate certificates. These certificates must be located on the certification chain between the server certificate and the server selected from list.

Server name –Enter the name of the authentication server.

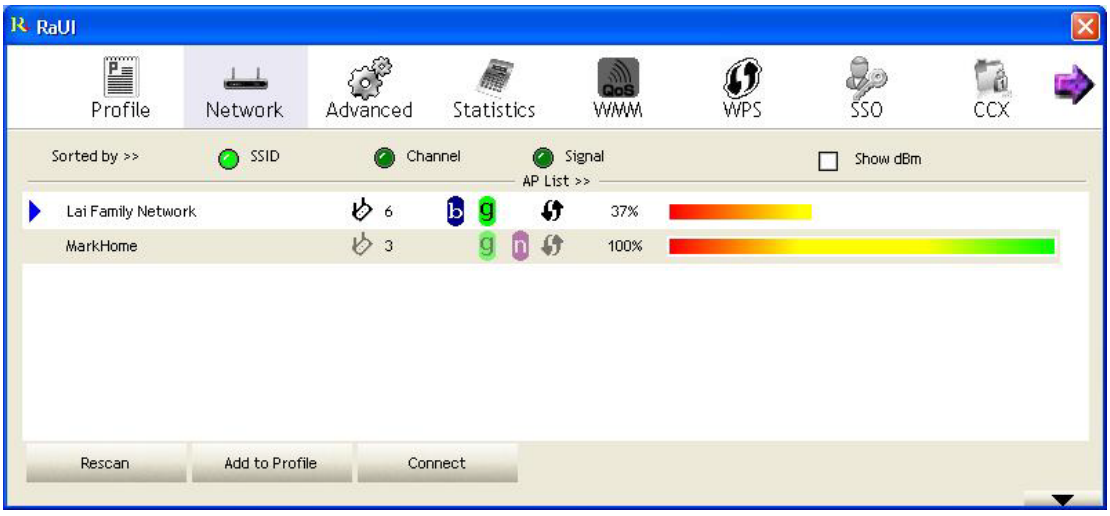
EAP-Fast Tab

Allow unauthenticated provision mode –During the PAC can be provisioned (distributed on time) to the client automatically. It only supported **Allow unauthenticated provision mode** and use **EAP-MSCHAP v2** authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even through it is made with an unknown server.

Use protected authentication credential –During the PAC can be provisioned to the client manually via disk or secured network distribution method. Click **Import**, to browse for PAC settings file or click **Remove**, to stop using current file.

File Path –A path where PAC setting file is located.

Network Tab



Icons on list means:

	Connection to this network established successfully
	Connection to this network not established
	Infrastructure type network
	Ad hoc type network
b g n	802.11 standards supported by wireless station
	Access Point supports WPS function and it's enabled
	Secured network

Show dBm – Check this box to show signal strength on **AP List** as dBm instead of percentages. This also applies to **Signal Strength** and **Noise Strength** in secondary pane.

AP List –List of wireless networks in range. Columns contain follow information: SSID (hidden when SSID Broadcast on AP is disabled), network type icon (infrastructure or Ad hoc) and used channel, supported 802.11 standards (i.e. 802.11g), security and signal strength. Double-click on network, to display detailed network information in secondary pane.

Rescan –Click this button to rescan for available wireless networks.

Add to Profile –Click to create a profile for selected network. You can find detailed information on profile configuration in previous section.

Connect –Click to connect to selected network without creating a profile.

Detailed network information

- **General Tab**

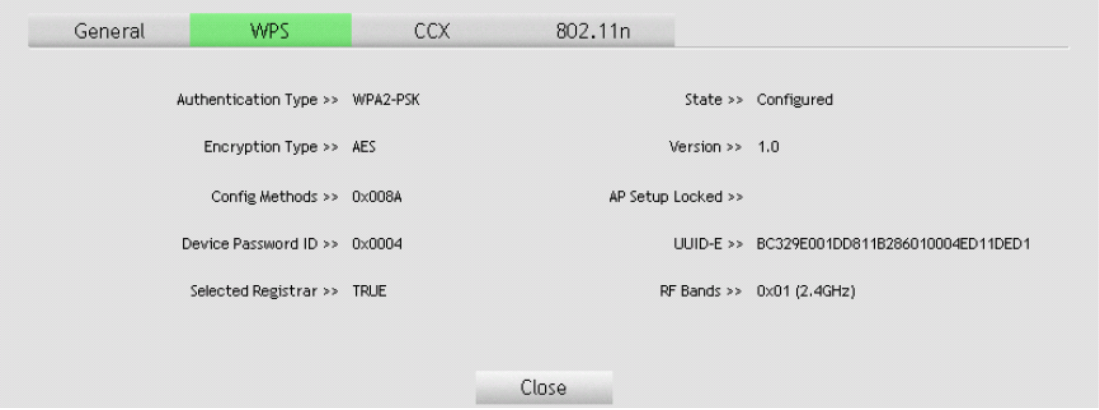
  General information on network and security.

General
WPS
CCX
802.11n
SSID >> PENTAGRAM P6431
MAC Address >> 00-04-ED-11-DE-D1
Authentication Type >> WPA2-PSK
Encryption Type >> TKIP
Channel >> 1 <--> 2412 MHz
Network Type >> Infrastructure
Beacon Interval >> 100
Signal Strength >> 100%
Legacy Supported Rates (Mbps): 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
802.11n Max. Supported Rates (Mbps): 300.0
Close

  SSID –Network SSID or Hidden if AP doesn't broadcast SSID.
  MAC Address –MAC address of AP.
  Authentication Type –Authentication used by this network.
  Encryption Type –Encryption used by this network.
  Channel –Channel and Frequency used by this network
  Network Type –Infrastructure or Ad-Hoc.
  Beacon Interval –Interval for sending beacon to sustain connection.

- **WPS Tab**

  Information on WPS (Wi-Fi Protected Setup)



  Authentication Type –There are three types of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.
  Encryption Type –For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and

WPA-PSK authentication mode, the encryption type supports both TKIP and AES.

Config Methods – Correspond to the methods that AP supports as an Enrollee for adding external Registrars (a bitwise or of values).

Value	Hardware Interface
0x0001	USBA (Flash Drive)
0x0002	Ethernet
0x0004	Label
0x0008	Display
0x0010	External NFC Token
0x0020	Integrated NFC Token
0x0040	NFC Interface
0x0080	Push Button
0x0100	Keypad

Device Password ID –Indicate the method or identifies the specific password that the selected Registrar intends to use. AP in PBC mode must indicate 0x0004 with two minute Walk Time.

Value	Description
0x0000	Default(PIN)
0x0001	User-specified
0x0002	Rekey
0x0003	Display
0x0004	Push Button (PBC)
0x0005	Registrar-specified
0x0006~0x000F	Integrated NFC Token

Selected Registrar –Indicate if the user has recently activated a Registrar to add an Enrollee. The values are **TRUE** and **FALSE**.

State –The current configuration state on AP. The values are **Unconfigured** and **Configured**.

Version –WPS specified version.

AP Setup Locked –Indicate if AP has entered a setup locked state.

UUID-E –The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes.

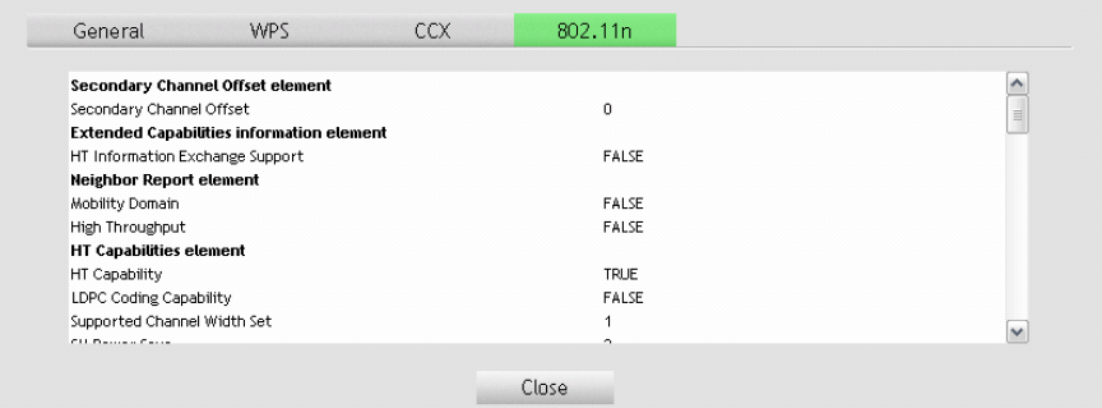
RF Bands –Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are **2.4GHz** and **5GHz**

- ## CCX Tab

Information regarding CCX (Cisco Compatible eXtensions) supported by AP.

- ## 802.11n Tab

Detailed information about APs support of 802.11n protocol and its functions. **FALSE** value means the function is not supported or disabled. **TRUE** means supported and enabled.



Advanced Tab

This Tab can be used to change advanced wireless network adapter options.

Wireless mode –Select wireless mode in which adapter will work.

Enable TX Burst –Selecting this mode may accelerate frame transmission.

Enable TCP Window Size –Selecting this feature may improve TCP performance on wireless connections.

Fast Roaming –Switchover between access points will occur when the current AP's minimum signal strength threshold set in this field is exceeded.

Show Authentication Status Dialog –When you connect AP with authentication, choose whether show **Authentication Status Dialog** or not. It displays the process about 802.1 x authentications.

Select Your Country Region Code –The item selected in this field determines the channels (frequencies) available. In some cases driver will select region based on regional settings of operating system – in those cases it's not possible to change this value.

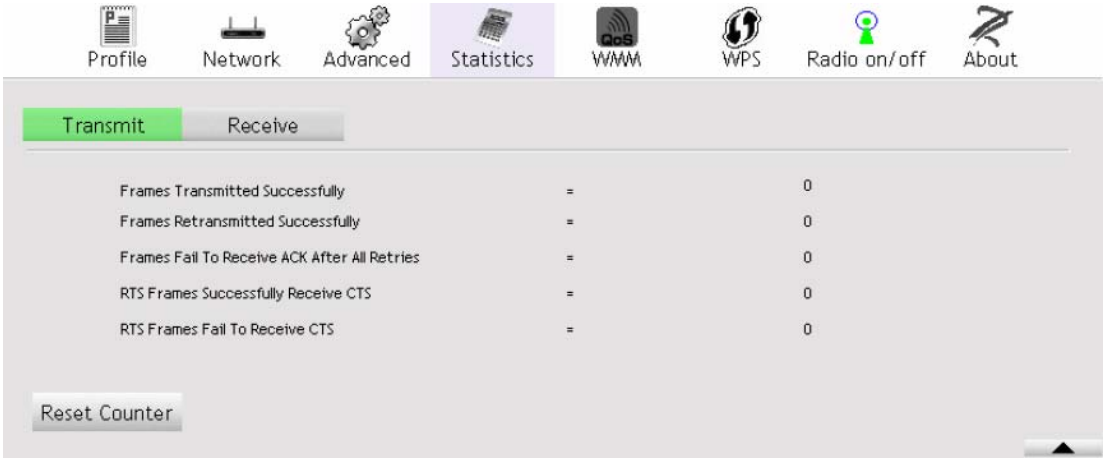
Enable CCX (Cisco Compatible eXtensions) –This enable supports for Cisco Compatible eXtensions:

- **Turn on CCKM** –Using LEAP allows taking advantage of CCKM (Cisco Centralized Key Management).
- **Enable Radio Measurement** –It supports for the Radio Measurement feature used in Cisco network hardware.

Apply –Apply changes.

Statistics Tab

This Tab shows Transmit and Receive statistics.



Frames Transmitted Successfully –shows the number of frames transmitted errors.

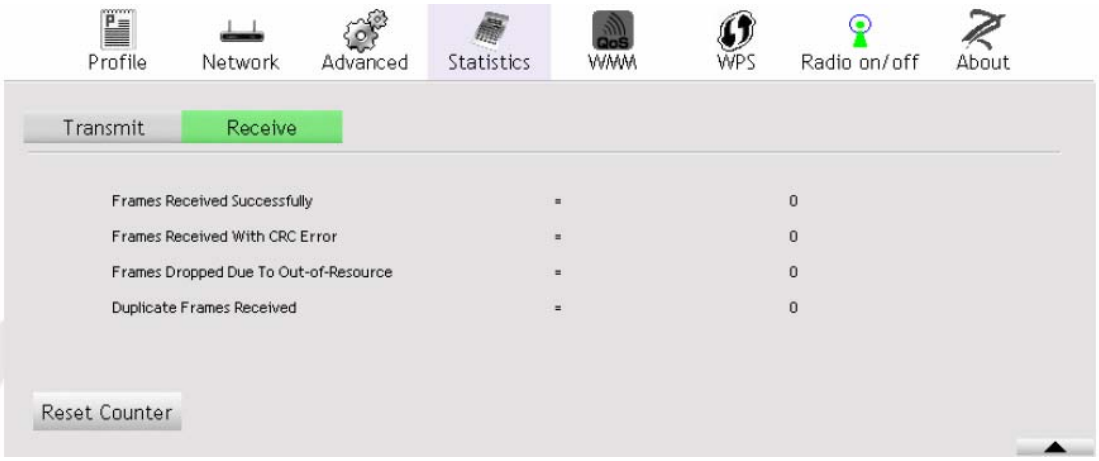
Frames Retransmitted Successfully –shows the number of frames transmitted successfully after retrying.

Frames Fail To Receive ACK After All Retries –shows the number of frames which did not receive acknowledgement after all retries.

RTS Frames Successfully Receive CTS –shows the number of RTS (Request To Send) frames which received responses in the form of CTS (Clear To Send) frames.

RTS Frames Fail To Receive CTS –shows the number of RTS (Request To Send) frames which did not received responses in the form of CTS (Clear To Send) frames.

Reset Counter – Click this button to reset all Transmit statistics.



Frames Received Successfully –shows the number of frames received without

errors.

Frames Received with CRC Error –shows the number of frames received with CRC errors.

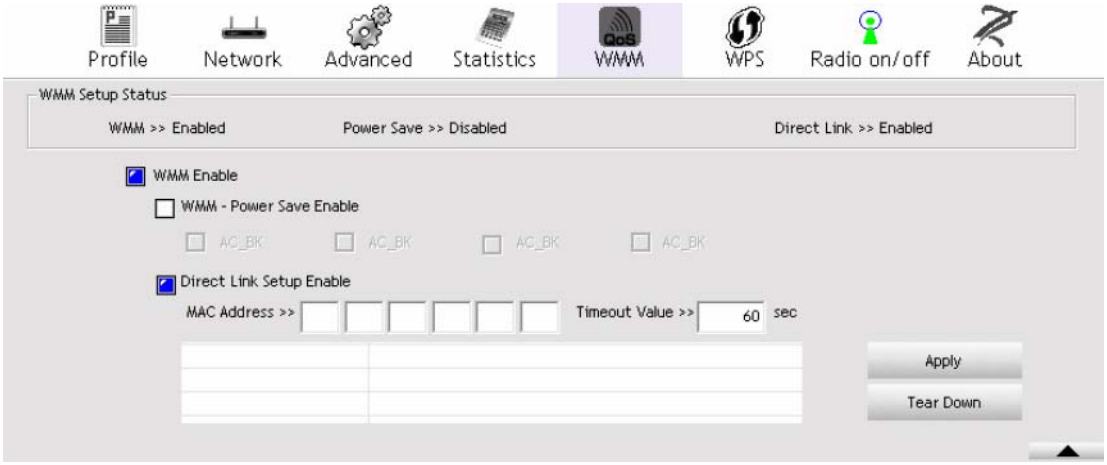
Frames Dropped Due To Out-of-Resource –shows the number of frames dropped due to resource issue.

Duplication Frames Received –show the number of duplicate frames received.

Reset Counter –Click this button to reset all Receive statistics.

WMM Tab

This Tab contains settings for WMM (Wi-Fi Multimedia), which provide basic QoS (Quality of Service) for 802.11 networks. WMM prioritize traffic base on four Access Categories (AC): Voice, Video, best effort and background. WMM doesn't guarantee throughput for ACs and can be used for VOIP applications. To use WMM functions WMM must be also supported by AP.



WMM Setup Status –Status of WMM option: **Disabled** or **Enabled**.
WMM Enable –Enable Wi-Fi Multi-Media.
WMM – **Power Save Enable** – Enable WMM Power Save and select ACs: AC_BK (background), AC_BE (best effort), AC_VI (Video), AC_VO (Voice).
Direct Link Setup Enable –Enable DLS (Direct Link Setup).
MAC address –MAC Address of remote STA (must conform to two conditions: connect with the same AP that support DLS features and have to enable DLS).
Timeout Value –represents that it disconnects automatically after some seconds. The value is integer. The integer must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is **60** seconds.
Apply –Click to save DLS and add it to the list.
Tear Down –Select DLS from list and click this button to remove it.

WPS Tab

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. Ralink STA as an Enrollee or external Registrar supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

WPS AP List –Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, Channel, ID (Device Password ID), and Security-Enable.

Rescan –issue a rescan command to wireless NIC to update information on surrounding wireless network.

Information –Displays information about WPS IE on the selected network. List information includes Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands. Details can be found in Detail network information section.

PIN Code –8-digi numbers. It is required to enter PIN Code into Registrar using method. When STA is Enrollee, you can use **Renew** button to re-generate new PIN Code.

Config Mode –Our station role-playing as an Enrollee or an external Registrar.

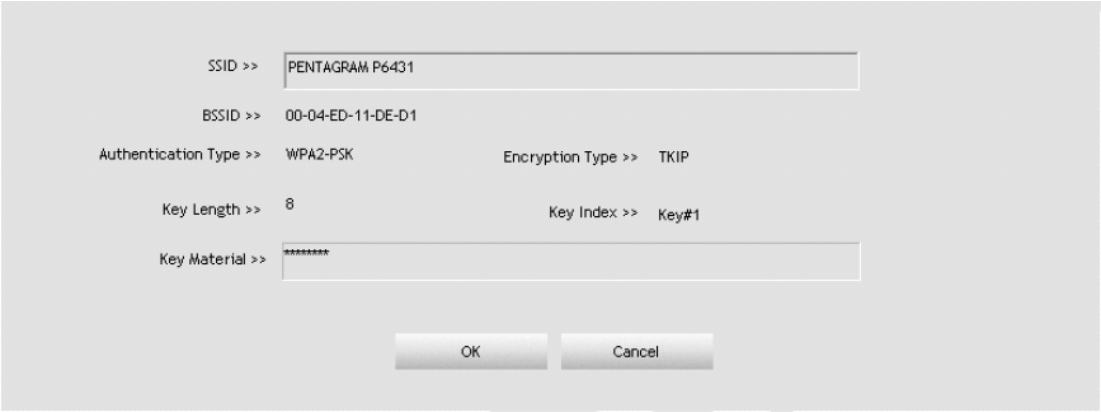
WPS Profile List –Display all of credentials got from the Registrar. List information includes SSID, MAC Address, Authentication and Encryption Type. If it's STA Enrollee, credentials are created as soon as each WPS success. If it's STA Registrar, RaUI creates a new credential with PA2-PSK/AES/64Hex-Key and doesn't change until next switching to STA Registrar.

Detail –Displays Credential information in secondary pane.

Connect –Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate –Command to rotate to connect to the next network inside credentials.
Disconnect –Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of RaUI if exists. If there is an empty profile page, the driver will select any non-security AP.
Export Profile –Export all credentials to Profile.
Delete –Delete an existing credential. And then select the next credential if exists. If there is an empty credential, the driver will select any non-security AP.
PIN –Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
PBC –Start to add to Registrar using PBC configuration method.
Caution: When you click **PIN** or **PBC,** please don't do any rescan within two-minute connection. If you want to abort this setup within the interval, restart **PIN**/**PBC** or click **Disconnect** to stop WPS action.
WPS Associate IE –Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE –Send the probe request with WPS IE during WPS setup. It is optional for STA.
Progress Bar –Display rate of progress from Start to Connected status.
Status Bar –Display currently WPS status.
Automatically select the AP –Start to add to AP by using to select the AP automatically in PIN method.

Credential information

Modification of these settings is possible only in Registrar mode.



SSID –Network SSID in credential.
BSSID –Network BSSID in credential.
Authentication Type –Authentication used by network in credential.
Encryption Type –Encryption used by network in credential.
Key Length –Encryption Key length.
Key Index –Encryption Key Index.
Key Material –Encryption Key.

Radio on/off Tab

Click this Tab to enable or disable radio transmission. Green icon –RF “On”, Red icon – RF “Off”.

About Tab

This Tab contains driver, application and network adapter information.

RaConfig Version –Shows the version of the RaConfig application.
Driver Version –Shows the current driver version.
Date –Shows the application/driver release date.
EEPROM Version –Shows the current EEPROM revision.
Firmware Version –Shows the current firmware version.
Phy_Address –Shows the adapter's physical address (MAC).

Troubleshooting

This chapter provides solutions to problems that may occur during the installation and operation of the wireless USB adapter.

1. **The Wireless USB Adapter does not work properly.**
   - Reinsert the Wireless Adapter into your PC's USB port.
   - Right click on **My Computer** and select **Properties**. Select the **device manger** and click on **Network Adapter**. You will find the Adapter if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of the Adapter. If there is a yellow question mark, please check the following:
   - Make sure that your PC has a free IRQ (Interrupt Request, a hardware interrupt on a PC).
   - Make sure that you have inserted the right adapter and installed the

proper driver. If the Adapter does not function after attempting the above steps, remove the adapter and do the following:

- Uninstall the driver software from your PC.
- Restart your PC and repeat the hardware and software installation as specified in this User Manual.

2. **I cannot communicate with other computers linked via Ethernet in the Infrastructure configuration.**
   - Make sure the power of the PC with Adapter associated is on.
   - Make sure that your Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.
3. **What should I do when the computer with the Adapter installed is unable to connect to the wireless network and/or the Internet?**
   - Check the LED indicators from the broadband modem, see if LED indicating normal activity. If not, there may be problem with the broadband connection.
   - Check the LED indicators on the wireless router or AP to see if they are functioning properly. If not, check if the AC power and Ethernet cable are firmly connected.
   - Check the IP address, subnet mask, gateway and DNS settings are correctly entered for the network.
   - In Infrastructure mode, make sure the same Service Set Identifier (SSID) is specified on the settings for the wireless clients and access points.
   - In Ad-Hoc mode, both wireless clients will need to have the same SSID. Please note that it might be necessary to set up one client to establish a BSS (Basic Service Set) and wait before setting up other clients. This prevents several clients from trying to establish a BSS at the same time, which can result in multiple singular BSSs being established, rather than a single BSS with multiple clients associated to it.
   - Check if the Network Connection for the wireless client is configured properly.
   - If Security is enabled, make sure the correct encryption keys are entered on both the Adapter and the access point.

Appendix A: Specification

Standards Compliance	IEEE 802.11b/g/n USB v1.0/1.1/2.0
Chipsets Solution	RT3070L
Frequency Band	America/FCC：2.412~2.462 GHz (11 channels) Europe CE/ETSI：2.412~2.472 GHz (13 channels) Japan : 2.412~2.484 GHz (14 channels)
Transmission Power	30dBm
Transmission Rate	IEEE802.11b: 11 Mbps IEEE802.11g: 54 Mbps IEEE802.11n 150 Mbps
Sensitivity	IEEE 802.11n: -90dBm @ HT20 IEEE 802.11g: -92dBm @ 54Mbps IEEE 802.11b: -95dBm @ 11Mbps
Antenna Type	External 4dBi Dipole Antenna(Optional)
Security Systems	64/128-bit WEP,WPA,WPA2,TKIP,AES,Cisco CCX,WAPI-CERT
USB	USB 2.0 with 5m cable
Temperature	32~122°F (0 ~50°C)
Network Management System OS Support	Windows 2000/XP/Vista, Windows 7, Linux, Mac X
Warranty	One year limited

FCC Notice

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and

2. This device must accept any interference received, including interference that may cause undesired operation.

Declaration of Conformity for RF Exposure

This device has been evaluated for RF exposure for Humans in reference to FCC radiation exposure limits set forth for an uncontrolled environment. The minimum separation distance from the antenna to human body is 20 cm.

IC Warning

This device complies with Industry Canada license-exempt RSS standard (s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Declaration of Conformity for RF Exposure

This device has been evaluated for RF exposure for Humans in reference to IC radiation exposure limits set forth for an uncontrolled environment. The minimum separation distance from the antenna to human body is 20 cm.

Déclaration de conformité de l'exposition RF

Ce périphérique a été évalué pour l'exposition humaine aux radiofréquences émises par référence à IC exposition en matière de radiations définies pour un environnement non contrôlé. La distance minimale de séparation de l'antenne de corps humain est de 20 cm.